REMARKS

Claims 1-3, 5-7, 9-11, 13-15 and 17-22 are now rejected under 35 USC 103(a) as being unpatentable over Forslow (US 2003/0039237 A1) in view of Borella et al. (US 6,697,354, newly cited). Claims 25 and 27-33 are now rejected under 35 USC 103(a) as being unpatentable over Leung (US 6,501,746) in view of Joong (US 6,549,776) and Borella et al.. These rejections are respectfully disagreed with and are traversed below.

As was previously argued, Forslow discloses the use of a common access server 118 at a GGSN 116 (e.g., paragraph [0078]). In a common authentication procedure (FIG. 12), if a PDP context has been requested by the mobile station, created, and accepted by the GGSN, the mobile station starts a common dynamic host configuration procedure (interleaved with the common authentication procedure) to establish a logical relationship to the GGSN by sending a DHCP Discover message providing the mobile station's unique identifier (MSid), a user identifier (Userid), a password, and other parameters that may be used to identify and authenticate the mobile station (paragraph [0097]).

The GGSN stores the mobile station's MSid (based on the IMSI), Userid, and password and proceeds with a common host configuration procedure. At this point a common authentication procedure with an ISP is completed for both circuit-switched and packet-switched bearer services (paragraph [0098]).

If a new application flow is started by the mobile station, rather than performing another authentication procedure involving the external ISP, the MSid, Userid, and password received in a PAP/CHAP request from the mobile station are compared to values stored in the common access server during the initial authentication procedure. If the received values match those stored in the access server, an authentication confirmation is transmitted as a CHAP/PAP response through the direct access unit at the MSC to the mobile station. The common access server matches the provided information with the stored information and authenticates the mobile without having to undertake another authentication procedure with the radius server in the ISP.

This same type of abbreviated authentication procedure is performed for other, subsequent application flows commenced during the session. (Paragraph [0100]).

The Examiner appears to be equating the common access server 118 of the GGSN 116 with the claimed subscriber database. While the Examiner's interpretation is not agreed with, the Examiner continues by equating the claimed "performing automated checking of a right of the terminal to use said subscriber database" with the disclosure in paragraphs [0100] and [0101].

As was previously argued, these paragraphs do not disclose the claimed subject matter. Even if one were to equate the claimed "subscriber database" with the mobile station information (MSid, Userid and password) stored by the GGSN in the common access server 118, which is not admitted is the case, there is no disclosure of "performing automated checking of a right of the terminal to use said subscriber database". Instead, what is disclosed (in paragraphs [0099] and [0100]) in part is simply that if one assumes that:

> ...a new application flow is started at the mobile station (e.g., an audio call from the mobile (party A) to a called party B) for which a circuit-switched bearer is selected....The direct access unit 112 then sends an authentication request to the common access server at the selected GGSN, shown in the FIG. 12 example in the form of a password authentication protocol (PAP) or challenge authentication protocol (CHAP) request, to forward the mobile station's authentication parameters including the MSid, Userid, and password to the common access server.... Rather than performing another authentication procedure involving the external ISP, the MSid, Userid, and password received in the PAP/CHAP request are compared to values stored in the common access server during the initial authentication procedure. **If the received values match those stored in the access server, an authentication confirmation is transmitted as a CHAP/PAP response through the direct access unit at the MSC to the mobile station. The common access server matches the provided information with the stored information and authenticates the mobile without having to undertake another authentication procedure with the radius server in the ISP.** This same type of abbreviated authentication procedure is performed for other, subsequent application flows commenced during the session.

Clearly, **this procedure does not suggest** "performing automated checking of a right of the terminal to use said subscriber database" (without admitting that the subscriber database is

equivalent to the mobile station information stored at the common access server), but instead suggests (at the most) authenticating a right of the mobile station to initiate the new application flow (an audio call in the example given by Forslow).

Clearly, the claimed element "performing automated checking of a right of the terminal to use said subscriber database" is not expressly or inherently described by Forslow, nor is it suggested by Forslow.

Further, the next element of claim 1 recites "automatically transmitting, from the subscriber database, subscriber data to the terminal, the serving network, or the terminal and the serving network, in response to the terminal having the right to use said subscriber database and in response to acceptable authentication of the subscriber database in the bearer network". There is no disclosure of this subject matter in paragraphs [0100]-[0105]. As was noted above, paragraph [0100] discloses that if "the received values match those stored in the access server, an authentication confirmation is transmitted as a CHAP/PAP response through the direct access unit at the MSC to the mobile station." Paragraph [0102] - [0105] variously disclose:

> The ISP 130 uses the subnet mask and giaddr to route a response back to the GGSN, which in turn, forwards the response to the mobile station based on the agent remote ID.....The DHCP server 134 in the ISP replies to the Discover message with an Offer message passed on by the GGSN relay agent 120 towards the mobile station including the "offered" configurations that the DHCP server 134 can provide (after checking the incoming and outgoing tunnel identifiers). Multiple offers can be received from various DHCP servers. The mobile station selects the DHCP offer that best satisfies its requirements and sends a DHCP request message to the DHCP server which provided the selected offer. The DCHP server then provides an IP address to the GGSN in a DHCP Acknowledgment message. The IP address is placed in a table along with the mobile's agent remote ID and agent circuit ID/tunnel identifier. The DHCP Acknowledge message is relayed to the mobile host which is configured with a set of selected DHCP parameters including IP address, DNS server name, etc. The common access server in the GGSN also stores these configuration parameters like the IP address allocated to the mobile station along with the authentication parameters like the MSid, Userid, password, etc.....If the mobile station initiates a new application flow over a circuit-switched bearer, i.e., in the example shown in FIG. 13 by sending a PPP Configure-Request via an L2TP

> tunnel to the GGSN, **the common access server compares the PPP Configure Request parameters including an MSid and default configuration parameters with the stored DHCP configuration information and returns an Acknowledgment if the comparison results in a match**. Another configuration operation with the ISP DHCP server is not required. **After this abbreviated configuration procedure, the common access server simply returns a PPP Configuration Acknowledgment via the direct access unit to the mobile station**, and the selected circuit-switched bearer commences transporting the desired information.

It is not seen where the various messages, etc. sent or returned to the mobile station of Forslow disclose "automatically transmitting, from the subscriber database, subscriber data to the terminal, the serving network, or the terminal and the serving network, in response to the terminal having the right to use said subscriber database and in response to acceptable authentication of the subscriber database in the bearer network", where the "subscriber data" is "similar to data stored in the subscriber application comprised by the terminal".

Further still, these acknowledgments sent from the common access server are clearly not disclosed as being sent "in response to the terminal having the right to use said subscriber database and in response to acceptable authentication of the subscriber database in the bearer network."

Instead, it appears that any mobile station related information stored at the common access server is simply used for making local, faster authentication decisions concerning the mobile station. There is no disclosure that any of this information is transmitted to the mobile station, or elsewhere for that matter. All that is said to be transmitted from the "common access server" is an **Acknowledgment** and a **PPP Configuration Acknowledgment**, not "subscriber data".

If the Examiner persists in rejecting the claims based on Forslow them he is respectfully requested to point out with more specificity exactly where he believes that Forslow actually discloses or suggests the claimed subject matter.

The Examiner correctly states that Forslow does not disclose "where an IP address of said

subscriber database is received from the terminal at the serving network and a connection is established from the terminal to said subscriber database on the basis of the IP address of said subscriber database". However, the Examiner cites Borella et al. for purportedly teaching this subject matter, and refers to col. 10, lines 7-40, col. 19, lines 36-67, and Figures 7, 8 and 15-19.

It is submitted that the teachings of Borella et al. do not cure the deficiencies in the teachings of Forslow.

First, the word "database" and the phrase "data base" do not appear in Borella et al. As such, it is not clear what elements of Borella et al. the Examiner is equating with the terminal sending an IP address of.

Borella et al. purport to disclose a distributed network address translation functionality for mobile network devices using locally-unique ports. In Borella et al. a mobile network device requests one or more locally-unique ports with a Port Allocation Protocol (PAP) from a second network device on a first network to identify the first network device on the first network if the mobile first network device roams to a second external network. One or more default or ephemeral ports on the mobile network device are replaced with one or more locally-unique ports obtained with the Port Allocation Protocol. The one or more locally-unique ports are said to allow the distributed network address translation to be used with the mobile network device, where a combination network address is created for the mobile network device with a locally unique port and an external network address for the first network to identify the mobile first network device if the mobile first network device roams to a second external network.

Col. 10, lines 7-40, states the following:

> FIG. 7 is a block diagram illustrating a combined network address layout 112 for combined network address 72. However, other layouts could also be used. Combined network address layout 112 includes a common external network address 114 such as an IP 48 address (e.g., common network address 28), and a globally unique port 116 or a locally-unique port for Mobile IP explained below,

obtained by sending a PAP request message 66 and receiving a PAP response message 68 from a network device. Network devices (14, 16, 18, 20, 22, 24) use combined network address 72 for communications with external second network 30 or third network 32. Common external network address 114 identifies first computer network 12 to an external second computer network (e.g., 30 or 32).

As is known in the art, to identify separate data streams, TCP 58 provides a source port field and a source address field in a TCP header. For more information on TCP headers see RFC-793. Since local or default port identifiers are selected independently by each TCP 58 stack in a network, they are typically not unique. To provide for unique addresses within each TCP 58, a local Internet address identifying TCP 58 can be concatenated with a local port identifier and a remote Internet address and a remote port identifier to create a "socket" that will be unique throughout all networks connected together. Sockets are known to those skilled in the networking arts.

In a preferred embodiment of the present invention, the source port in a header is given a globally unique port obtained with PAP 64 and given a common external network address. Together they uniquely identify applications and protocols on network devices (14, 16, 18, 20, 22, 24) on first computer network 12 to second external computer network (e.g., 30 or 32) with a value conceptually similar to the socket used by TCP 58.

Col. 19, line 36, to col. 10, line 4, states as follows:

As is illustrated in FIG. 15, the mobile node 210 has a network address (e.g., IP 48 address) of 11.0.0.4 on the home subnet 212. The home agent 208 has a network address of 11.0.0.7 on the home subnet 212. The mobile node 210 with network address 11.0.0.4, belongs to the home subnet 212 with network access prefix of 11.0.0 and a prefix length of 24 bits (i.e., 11.0.0.X/24). Network devices on the home subnet 212 have network addresses beginning with the network access prefix of 11.0.0 and a prefix length of 24 bits. Since the home agent 208 is advertising a route to the home subnet 212 at 11.0.0.X/24, it will accept data packets from external network 214 for network addresses with the network access prefix 11.0.0.X/24. For example, the home agent 208 accepts data packets for the mobile node 210 that has a home network address of 11.0.0.4, where X=4 since the network access prefix is equal to 11.0.0 with a length of 24-bits.

The foreign agent 216 has a network address of 12.0.0.4 on the foreign subnet 218. The foreign agent advertises a route to the foreign subnet 218 with network access prefix/prefix length of 12.0.0.Y/24. The foreign agent 216 will accept data packets that have a network address of 12.0.0.Y/24 on the foreign subnet 218. For

> example, the foreign agent will accept data packets for the computer 220 with a network address of 12.0.0.1, where Y=1, since the network access prefix is equal to 12.0.0 with a length of 24-bits.
>
> The mobile node 210 uses its home network address of 11.0.0.4 on the home subnet 212 to register with the foreign agent 216 and the home agent 208. After registration of the mobile node 210, the foreign agent 216 will also accept data packets for the mobile node 210 at the specific home network address 11.0.0.4/ for the mobile mode 210 as well as data packets that have a network prefix of 12.0.0/24. The foreign agent 216 also assigns a temporary foreign network address on the foreign subnet 218 to the mobile node 210 (e.g., 12.0.0.5).

It is not understood where the Examiner finds in these portions of Borella et al. any express disclosure, or even a suggestion of: "**where an IP address of said subscriber database is received from the terminal at the serving network and a connection is established from the terminal to said subscriber database on the basis of the IP address of said subscriber database**". Basically all that is stated is that the mobile node 210 uses its home network address on the home subnet to register with the foreign agent and the home agent.

Further, it is not admitted that Forslow (who discloses the use of the common access server at a GGSN to accomplish a common authentication procedure for a mobile station) and Borella et al. (who disclose distributed network address translation functionality for mobile network devices using locally-unique ports) are in the "same field of endeavor".

It is further not admitted that "it would have been obvious to one of ordinary skill in the art" to somehow attempt to combine the teachings of Forslow and Borella et al.

It is further not admitted, even if Forslow and Borella et al. were to be somehow combined, which is clearly not admitted is suggested or even technically feasible, that the subject matter found in claim 1 would be suggested to, or found obvious by, one of ordinary skill in the art.

In that claim 1 is clearly not rendered unpatentable by the Examiner's proposed combination of Forslow and Borella et al., then for at least this one reason all claims that depend from claim 1

are also in condition for immediate allowance.

The arguments advanced above with respect to claim 1 apply as well to independent claim 13, which was previously amended in a similar manner. In that claim 13 is not rendered unpatentable by the Examiner's proposed combination of Forslow and Borella et al., then all claims that depend from claim 13 are also allowable for at least this one reason.

If the Examiner persists in rejecting claims 1-3, 5-7, 9-11, 13-15 and 17-22 in a final rejection based on Forslow in view of Borella et al. then he is respectfully requested to point out with more specificity exactly where he believes that the combination of Forslow with Borella et al. actually discloses or suggests the claimed subject matter. As was shown above, the rationale for such a rejection is simply not supported by a reading of either Forslow or Borella et al.

Turning now to the rejection of claims 25 and 27-33 under 35 USC 103(a) as being unpatentable over Leung in view of Joong and Borella et al., this rejection is also traversed.

The arguments made in the prior response are repeated and incorporated by reference herein.

Leung fails to disclose the currently claimed use of a subscriber application, such as a SIM of a GSM terminal, comprised by the terminal. The cited portions of Leung only disclose the general transmission of a Mobile IP registration request.

As was argued previously, Leung relates simply to IP address assignment in a Mobile IP system. In particular, Leung is directed to assigning an IP address to a mobile node during registration which is accomplished by mapping a mobile node ID (associated with the mobile node) to an assigned IP address. A registration request is sent by the mobile node to a Home Agent. Once an IP address is assigned to the mobile node, the IP address may be transferred to the mobile node in a registration reply composed by the Home Agent.

The use of Joong for purportedly teaching a subscriber database with a functional connection to a

bearer network, where subscriber data is similar to data stored in a subscriber application of the terminal, where the subscriber data includes "authentication information" (which is clearly not admitted is the case), does not remedy the deficiencies in the teachings of Leung. As was noted above, the cited disclosure in col. 5 of Joong is simply related to a WAP gateway transmitting a location request to determine a serving mobile switching center MSC 120 and MSC/VLR location area 117 for a wireless client 105.

The Examiner relies several times on col. 7, lines 5-30, of Leung. What is actually stated at col. 6, line 66 to col. 7, line 55 is as follows:

> Once the care-of address has been obtained, a registration request is composed and sent via the care-of address at step 208. As described above, the mobile node may have a mobile node ID (e.g., serial number) that identifies the mobile node. In order that the mobile node may be identified by data contained in the registration request, at least a portion of the mobile node ID is obtained and provided in the registration request. Typically, the IP address, or Home Address, of the mobile node is provided in a Home Address field of the registration request. In the absence of an IP address, this field may be used to store the mobile node ID or a portion thereof. Thus, assuming that the mobile node ID contains a number of bytes less than or equal to that of the Home Address field, the mobile node ID may be provided in the Home Address field of the registration request packet. Alternatively, a portion of the mobile node ID may be provided in the Home Address field where the size of the mobile node ID is greater than that of the Home Address field. In order to indicate that the mobile node needs an IP address, the registration request may include an ID indicator that may be used for this purpose. By way of example, the ID indicator may include an ID bit which indicates that the mobile node has an IP address when the ID bit is in a first state, and otherwise indicates that the mobile node does not have an IP address. The ID bit may be one of the reserved bits of the registration request packet.
>
> Once composed, the registration request is sent via the care-of address. If there is a foreign agent, the registration request is sent via the foreign agent care-of address. Alternatively, after the collocated care-of address is obtained at step 206, the registration request is composed and sent via the collocated care-of address.
>
> Once the registration request is sent (via Foreign Agent care-of address or collocated care-of address), it is received by the Home Agent associated with the mobile node at step 210. As described above, the registration request comprises a registration request packet that includes at least a portion of the mobile node ID.

> Next, at step 212, it is determined whether the registration is authenticated by the Home Agent, as provided by RFC 2002 for example. Authentication is typically performed using the Home Address field of the registration request. However, as will be described with reference to FIGS. 12-16A, in the case where the size of the mobile node ID is greater than the Home Address field and a portion of the mobile node ID is not guaranteed to be unique, the mobile node ID may be used for authentication purposes. At step 214, if the registration is not authenticated, the mobile node is not registered with the Home Agent and the process is complete as indicated at step 216.
>
> If the registration is authenticated, registration is completed by the Home Agent in steps 218 through 232. The Home Agent verifies if the mobile node needs an IP address at step 218. According to the first embodiment, the Home Agent checks the ID indicator of the registration request to obtain this information. The process flow then diverges at step 220 depending upon whether the mobile node needs an IP address.

The subject matter of claim 25 is not seen to expressly disclosed or suggested, nor is it suggested by col. 11-lines 4-65, col. 12, lines 1-40, or col. 14, lines 7-14.

As regards Joong, it does not teach the above-indicated further features not disclosed by Leung. Furthermore, Joong fails to disclose the claimed subscriber database comprising subscriber data similar to data stored in a subscriber application comprised by the terminal, and subscriber data including authentication information. The cited disclosure in col. 5 is simply related to a WAP gateway transmitting a location request to determine a serving mobile switching center MSC 120 and MSC/VLR location area 117 for a wireless client 105.

As such, even if Leung and Joong were to be combined, which is not admitted is suggested or feasible, the resulting combination would still not teach or suggest the claimed subject matter.

The Examiner acknowledges that Leung and Joong do not teach:

> where said terminal device contains an IP address of the subscriber database and transmits the IP address to the serving network, and where a connection is established from the terminal device to the subscriber database on the basis of the IP address of the subscriber database,

and has applied Borella et al. referring again to col. 10, lines 7-40, col. 19, lines 36-67, and Figures 7, 8 and 15-19.

For all of the reasons argued above, it is respectfully submitted that the teachings of Borella et al. do not cure the deficiencies in the teachings of Leung and Joong. Claim 25 is clearly allowable, and all claims that depend from claim 25 are allowable for at least this one reason.

The arguments made above apply equally to claim 31. Claim 31 recites in part "where an IP address of the subscriber database is received from the terminal and is used to establish a connection between the terminal to the subscriber database".

For all of the reasons argued above, it is respectfully submitted that the teachings of Borella et al. do not cure the deficiencies in the teachings of Leung and Joong. Claim 31 is clearly allowable, and all claims that depend from claim 31 are allowable for at least this one reason.

The Examiner is respectfully requested to reconsider and remove the rejections of the claims under 35 U.S.C. 103(a) based on Forslow and Borella et al, and those based on Leung in view of Joong and Borella et al., and to allow all of the pending claims as presented for examination. An early notification of the allowability of all of the pending claims is earnestly solicited.

If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at the number provided.

S.N.: 10/082,348
Art Unit: 2617

Respectfully submitted:

Harry F. Smith
Reg. No.: 32,493

1/25/2011
Date

Customer No.: 10948

HARRINGTON & SMITH, Attorneys At Law, LLC
4 Research Drive
Shelton, CT 06484-6212

Telephone: (203)925-9400 ext. 15
Facsimile: (203)944-0245
email: hsmith@hspatent.com

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. BOX 1450, Alexandria, VA 22313-1450.

1-25-2011
Date

Claire F. Mason
Name of Person Making Deposit